PATENT ABSTRACTS OF JAPAN

AB

(11)Publication number : 2002-124960
(43)Date of publication of application : 26.04.2002

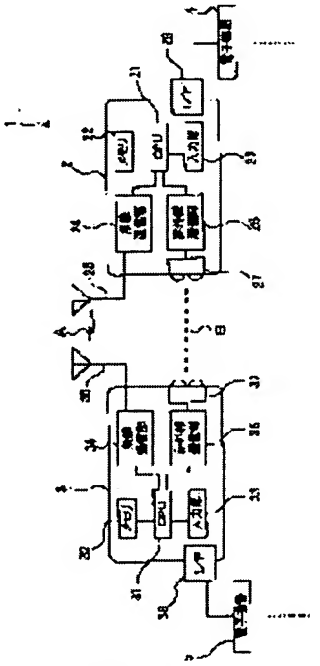
(51)Int.Cl. H04L 12/28
H04L 9/08

(21)Application number : 2000-315395
(22)Date of filing : 16.10.2000

(71)Applicant : LINK EVOLUTION CORP
(72)Inventor : KITAKADO KENTARO

(54) COMMUNICATION DEVICE, COMMUNICATION SYSTEM, AND COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To improve reliability in security without losing the convenience of radio communication when transmitting or receiving data between a plurality of electronic equipment by radio communication.
SOLUTION: In a communication system 1, data are transmitted or received via a radio communication link A conforming to the Bluetooth standard and an infrared communication link B between communication devices 2 and 3. The communication device 2 transmits original encryption information retained in a memory 22 to the communication device 3 via the infrared communication link B, and the communication device 3 retains the transmitted original encryption information in a memory 32. Then, when information is to be transmitted via the radio communication link A from the communication device 2 to the communication device 3, information that is encrypted based on the original encryption information in the memory 22 is transmitted.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－124960
（P2002－124960A）
(43)公開日　平成14年４月26日(2002.4.26)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/00	３１０Ｂ	５Ｊ１０４
9/08		9/00	６０１Ｃ	５Ｋ０３３

審査請求　未請求　請求項の数８　ＯＬ　（全 14 頁）

(21)出願番号　特願2000－315395(P2000－315395)

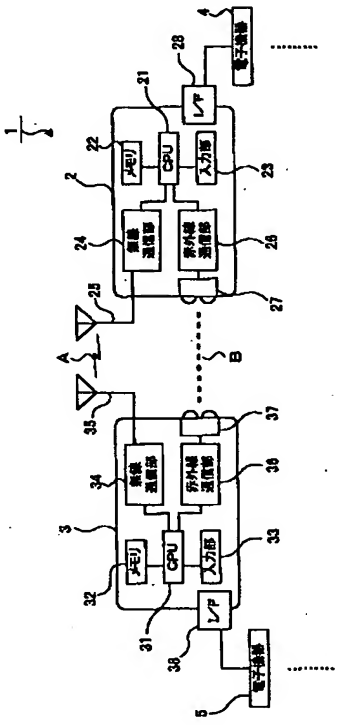
(22)出願日　平成12年10月16日(2000.10.16)

(71)出願人　500225837
リンク・エボリューション株式会社
東京都世田谷区松原３丁目40番７号
(72)発明者　北角　権太郎
東京都世田谷区松原３丁目40番７号　リンク・エボリューション株式会社内
(74)代理人　100090033
弁理士　荒船　博司　（外１名）

Ｆターム(参考)　5J104 AA16 EA04 EA21 NA02 NA37
5K033 AA08 CB06 DA17 DA20

(54)【発明の名称】　通信装置、通信システム、及び、通信方法

(57)【要約】
【課題】　複数の電子機器間で無線通信によってデータを送受信する場合に、無線通信の利便性を損なうことなくセキュリティ上の信頼性を向上させる。
【解決手段】　通信装置２と通信装置３との間において、Bluetooth規格に準じた無線通信リンクＡと、赤外線通信リンクＢとを介してデータを送受信する通信システム１であって、通信装置２は、メモリ２２内に保持する原始暗号化情報を、赤外線通信リンクＢを介して通信装置３へ送信し、通信装置３は、送信された原始暗号化情報を受信してメモリ３２内に保持する。そして、通信装置２から通信装置３へ無線通信リンクＡを介して情報を送信する場合は、メモリ２２内の原始暗号化情報に基づいて暗号化した情報を送信する。



1

【特許請求の範囲】

【請求項１】無線信号を送受信する第１の通信手段と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段と、

暗号化鍵情報を保持する鍵情報保持手段と、

この鍵情報保持手段に保持された暗号化鍵情報を、前記第２の通信手段によって他の通信装置へ送信させる鍵情報送信制御手段と、

前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって送信させる通信制御手段と、

を備えることを特徴とする通信装置。

【請求項２】前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、前記第１の通信手段による無線信号の送受信を拒否する通信拒否手段をさらに備えることを特徴とする請求項１記載の通信装置。

【請求項３】前記第１の通信手段はブルートゥース規格に準じた通信方式により無線信号を送受信するものであって、

前記第２の通信手段は、赤外線信号を用いた通信方式により無線信号を送受信することを特徴とする請求項１または２記載の通信装置。

【請求項４】送信側装置と受信側装置とを備えてなる通信システムであって、

前記送信側装置は、

無線信号を送受信する第１の通信手段と、

この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段と、

暗号化鍵情報を保持する鍵情報保持手段と、

この鍵情報保持手段に保持された暗号化鍵情報を、前記第２の通信手段によって前記受信側装置へ送信させる鍵情報送信制御手段と、

前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって前記受信側装置へ送信させる通信制御手段とを備え、前記受信側装置は、

前記送信側装置が有する第２の通信手段により送信された暗号化鍵情報を受信する鍵情報受信手段と、

この鍵情報受信手段により受信された暗号化鍵情報を保持する受信鍵情報保持手段と、

前記送信側装置が有する第１の通信手段により送信された情報を受信する暗号化情報受信手段とを備えること、

を特徴とする通信システム。

【請求項５】前記送信側装置は、前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、前記受信側装置が有する受信鍵情報保持手段に保持されていない場合に、前記第１の通信手段による無線信号の送受信を拒否する通信拒否手段をさらに備えることを特徴とする請求項４記載の通信システム。

2

【請求項６】前記送信側装置が有する第１の通信手段と、前記受信側装置が有する暗号化情報受信手段とは、ブルートゥース規格に準じた通信方式により無線信号を送受信するものであって、

前記送信側装置が有する前記第２の通信手段と、前記受信側装置が有する鍵情報受信手段とは、赤外線信号を用いた通信方式により無線信号を送受信することを特徴とする請求項４または５記載の通信システム。

【請求項７】前記送信側装置が有する鍵情報送信制御手段は、前記暗号化鍵情報を暗号化して前記第２の通信手段によって送信させることを特徴とする請求項４から６のいずれかに記載の通信システム。

【請求項８】無線信号を送受信する第１の通信手段と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段とを有する送信側装置と、受信側装置とを備えてなる通信システムにおける通信方法であって、

前記送信側装置により、暗号化鍵情報を前記第２の通信手段によって前記受信側装置へ送信する工程と、

前記受信側装置により、前記送信側装置が有する第２の通信手段により送信された暗号化鍵情報を受信して記憶する工程と、

前記送信側装置により、前記暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって前記受信側装置へ送信する工程と、

を含むことを特徴とする通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、異なる複数の通信方式に対応する通信装置、この通信装置を備える通信システム、及び、この通信システムにおける通信方法に関する。

【０００２】

【従来の技術】従来、パーソナルコンピュータ、ＰＤＡ（Personal Digital Assistant）、携帯電話機等の電子機器間でデータ通信を行う場合には、互いの電子機器をケーブルで接続する手法が用いられていた。しかし、ケーブルを用いた手法は、電子機器にケーブルを接続する手間がかかり、ケーブルを携帯しなければならないため、不便であった。そこで、最近では、複数の電子機器間におけるデータ通信に無線通信技術が用いられるようになった。

【０００３】特に、近年では、電子機器の利便性を向上させるため、互換性に富む複数の無線通信規格が策定されている。これらの通信規格に準じた通信装置を用いれば、様々な電子機器との間でデータ通信を容易に行うことができる。

【０００４】

【発明が解決しようとする課題】しかしながら、無線通信技術を利用してデータ通信を行う場合は、データの漏

洩に注意する必要があった。特に、様々な機器との間で通信可能な通信規格に準じている場合は、誤って無関係な他の機器によってデータが受信されないように注意する必要があった。このように、無線通信技術を用いたデータ通信では、セキュリティ上の信頼性を向上することが課題となっていた。

【０００５】本発明の課題は、複数の電子機器間で無線通信によってデータを送受信する場合に、無線通信の利便性を損なうことなくセキュリティ上の信頼性を向上させることである。

【０００６】

【課題を解決するための手段】本発明は、このような課題を解決するために、次のような特徴を備えている。なお、次に示す手段の説明中、括弧書きにより実施の形態に対応する構成を一例として示す。符号等は、後述する図面参照符号等である。

【０００７】請求項１記載の発明の通信装置（２）は、無線信号を送受信する第１の通信手段（例えば、図１に示す無線通信部２４）と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段（例えば、図１に示す赤外線通信部２６）と、暗号化鍵情報を保持する鍵情報保持手段（例えば、図２に示す原始暗号化情報格納領域１０１を有するメモリ２２）と、この鍵情報保持手段に保持された暗号化鍵情報を、前記第２の通信手段によって他の通信装置へ送信させる鍵情報送信制御手段（例えば、図３（ａ）に示す処理を行うＣＰＵ２１）と、前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって送信させる通信制御手段（例えば、図５に示す処理を行うＣＰＵ２１）とを備えることを特徴とする。

【０００８】この請求項１記載の発明によれば、無線信号を送受信する第１の通信手段と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段とを備え、鍵情報保持手段により、暗号化鍵情報を保持し、この鍵情報保持手段に保持された暗号化鍵情報を、鍵情報送信制御手段の制御により、第２の通信手段によって他の通信装置へ送信するとともに、通信制御手段の制御によって、鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、第１の通信手段によって送信するので、この通信装置により送信される情報は、第２の通信手段によって送信された暗号化鍵情報を受信した通信装置でのみ受信することができる。これにより、第１の通信手段による無線通信について、セキュリティ上の信頼性を確保することができる。特に、第１の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により情報が受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第２の通信手段によって送信される暗号化鍵情報を受信した通信装置のみに限定できる。従って、通信相手の装置との位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

【０００９】請求項２記載の発明は、請求項１記載の通信装置において、前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、前記第１の通信手段による無線信号の送受信を拒否する通信拒否手段（例えば、図５のステップＳ４５に示す処理を行うＣＰＵ２１）をさらに備えることを特徴とする。

【００１０】請求項２記載の発明によれば、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、通信拒否手段により、第１の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置を厳格に限定し、情報の秘匿をより確実に保持することができる。

【００１１】請求項３記載の発明は、請求項１または２記載の通信装置において、前記第１の通信手段はブルートゥース（Bluetooth）規格に準じた通信方式により無線信号を送受信するものであって、前記第２の通信手段は、赤外線信号を用いた通信方式により無線信号を送受信することを特徴とする。

【００１２】請求項３記載の発明によれば、第１の通信手段はブルートゥース（Bluetooth）規格に準じた通信方式により無線信号を送受信するものであり、第２の通信手段は、赤外線信号を用いた通信方式により無線信号を送受信するので、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース（Bluetooth）規格の無線通信において、情報の秘匿性を確保することができる。特に、第２の通信手段に赤外線信号を用いた通信方式を利用するので、第２の通信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能である。また、赤外線信号を用いた通信方式では、通信装置は互いに近接し、かつ所定の立体角以内で対向する必要があるので、情報の秘匿性をより一層高めることができる。

【００１３】請求項４記載の発明は、送信側装置（例えば、図１に示す通信装置２）と受信側装置（例えば、図１に示す通信装置３）とを備えてなる通信システム（１）であって、前記送信側装置は、無線信号を送受信する第１の通信手段（例えば、図１に示す無線通信部２４）と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段（例えば、図１に示す赤外線通信部２６）と、暗号化鍵情報を保持する鍵情報保持手段（例えば、図２に示す原始暗号化情報格納領域１０１を有するメモリ２２）と、この鍵情報保持手段に保持された暗号化鍵情報を、前記第２の通信手段によって前記受信側装置へ送信させる鍵情報送信制御手段（例

えば、図３（ａ）に示す処理を行うＣＰＵ２１）と、前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって前記受信側装置へ送信させる通信制御手段（例えば、図５に示す処理を行うＣＰＵ２１）とを備え、前記受信側装置は、前記送信側装置が有する第２の通信手段により送信された暗号化鍵情報を受信する鍵情報受信手段（例えば、図１に示す赤外線通信部３６、及び図３（ｂ）に示す処理を行うＣＰＵ３１）と、この鍵情報受信手段により受信された暗号化鍵情報を保持する受信鍵情報保持手段（例えば、図１に示すメモリ３２）と、前記送信側装置が有する第１の通信手段により送信された情報を受信する暗号化情報受信手段（例えば、図１に示す無線通信部３４）とを備えることを特徴とする。

【００１４】請求項４記載の発明によれば、送信側装置と受信側装置とを備えてなる通信システムであって、送信側装置は、無線信号を送受信する第１の通信手段と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段とを備え、鍵情報保持手段により暗号化鍵情報を保持し、鍵情報保持手段に保持された暗号化鍵情報を、鍵情報送信制御手段によって、第２の通信手段によって受信側装置へ送信させるとともに、通信制御手段の制御によって、鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、第１の通信手段によって受信側装置へ送信し、受信側装置は、送信側装置が有する第２の通信手段により送信された暗号化鍵情報を鍵情報受信手段によって受信し、鍵情報受信手段により受信された暗号化鍵情報を受信鍵情報保持手段によって保持し、送信側装置が有する第１の通信手段により送信された情報を暗号化情報受信手段によって受信する。

【００１５】また、請求項８記載の発明は、無線信号を送受信する第１の通信手段（例えば、図１に示す無線通信部２４）と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段（例えば、図１に示す赤外線通信部２６）とを有する送信側装置（例えば、図１に示す通信装置２）と、受信側装置（例えば、図１に示す通信装置３）とを備えてなる通信システム（１）における通信方法であって、前記送信側装置により、暗号化鍵情報を前記第２の通信手段によって前記受信側装置へ送信する工程と、前記受信側装置により、前記送信側装置が有する第２の通信手段により送信された暗号化鍵情報を受信して記憶する工程と、前記送信側装置により、前記暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって前記受信側装置へ送信する工程とを含むことを特徴とする。

【００１６】従って、送信側装置により送信される情報は受信側装置でのみ受信することができる。これにより、送信側装置が有する第１の通信手段を用いた通信システム内の無線通信について、セキュリティ上の信頼性を確保することができる。特に、第１の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第２の通信手段によって送信される暗号化鍵情報を保持する受信側装置のみに限定できる。従って、互いの装置の位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

【００１７】請求項５記載の発明は、請求項４記載の通信システムにおいて、前記送信側装置は、前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、前記受信側装置が有する受信鍵情報保持手段に保持されていない場合に、前記第１の通信手段による無線信号の送受信を拒否する通信拒否手段（例えば、図５のステップＳ４５に示す処理を行うＣＰＵ２１）をさらに備えることを特徴とする。

【００１８】請求項５記載の発明によれば、送信側装置は、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、受信側装置が有する受信鍵情報保持手段に保持されていない場合に、通信拒否手段によって、第１の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置をより厳格に限定し、情報の秘匿をより確実に保持することができる。

【００１９】請求項６記載の発明は、請求項４または５記載の通信システムにおいて、前記送信側装置が有する第１の通信手段と、前記受信側装置が有する暗号化情報受信手段とは、ブルートゥース（Bluetooth）規格に準じた通信方式により無線信号を送受信するものであって、前記送信側装置が有する前記第２の通信手段と、前記受信側装置が有する鍵情報受信手段とは、赤外線信号を用いた通信方式により無線信号を送受信することを特徴とする。

【００２０】請求項６記載の発明によれば、送信側装置が有する第１の通信手段と、受信側装置が有する暗号化情報受信手段とは、ブルートゥース（Bluetooth）規格に準じた通信方式により無線信号を送受信するものであって、送信側装置が有する第２の通信手段と、受信側装置が有する鍵情報受信手段とは、赤外線信号を用いた通信方式により無線信号を送受信するので、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース（Bluetooth）規格の無線通信において、情報の秘匿性を確保することができる。特に、第２の通信手段と鍵情報受信手段とは赤外線信号を用いた通信方式を利用するので、第２の通信手段および鍵情報受信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能である。また、赤外線信号を用いた通信方式では、送信側装置と受信側装置とは互いに

近接し、かつ所定の立体角以内で対向する必要があるので、情報の秘匿性をより一層高めることができる。

【００２１】請求項７記載の発明は、請求項４から６のいずれかに記載の通信システムにおいて、前記送信側装置が有する鍵情報送信制御手段は、前記暗号化鍵情報を暗号化して前記第２の通信手段によって送信させることを特徴とする。

【００２２】請求項７記載の発明によれば、送信側装置が有する鍵情報送信制御手段は、暗号化鍵情報を暗号化して第２の通信手段によって送信させるので、暗号化鍵情報を送信する際の情報の漏洩をより確実に防止できる。これにより、セキュリティ上の信頼性をより一層高めることができる。

【００２３】

【発明の実施の形態】以下、図を参照して本発明の実施の形態を詳細に説明する。

【００２４】〔第１の実施の形態〕図１は、本発明を適用した第１の実施の形態としての通信システム１の構成を示すブロック図である。同図に示すように、通信システム１は、互いに通信可能な通信装置２及び通信装置３により構成される。通信装置２と通信装置３との間には、無線電波を媒体とする無線通信リンクＡと、赤外線を利用した赤外線通信リンクＢとが形成される。

【００２５】なお、図１に示す通信装置２及び通信装置３は、いずれも同一構成によってなる通信装置であるが、本第１の実施の形態においては、通信装置２をアクセス要求側の装置、通信装置３をアクセス受信側の装置として説明する。

【００２６】通信装置２は、ＣＰＵ（Central Processing Unit）２１、メモリ２２、入力部２３、無線通信部２４、アンテナ２５、赤外線通信部２６、赤外線受発光ユニット２７、及びインターフェース部２８の各部を備えて構成される。

【００２７】ＣＰＵ２１は、入力部２３における指示操作に従って、メモリ２２に格納されたシステムプログラムを読み出して実行し、通信装置２の各部を駆動制御する。具体的には、ＣＰＵ２１は、メモリ２２内のプログラムに従って、無線通信部２４を制御し、通信装置３との間に無線通信リンクＡを確立する。続いてＣＰＵ２１は、赤外線通信部２６及び赤外線受発光ユニット２７によって赤外線通信リンクＢを確立する。そして、ＣＰＵ２１は、赤外線通信リンクＢを介して、メモリ２２内に格納された暗号化に関する各種情報を通信装置３へ送信する。

【００２８】その後、ＣＰＵ２１は、通信装置３から赤外線通信リンクＢを介して送信された情報を受信し、情報の内容を確認して、通信装置３との間の無線通信リンクＡ及び赤外線通信リンクＢを切断する。

【００２９】また、ＣＰＵ２１は、入力部２３から入力される指示に従って、無線通信部２４を制御し、通信装置２の近辺に存在する通信装置をスキャンするための無線信号をアンテナ２５から出力させる。このスキャン動作により、無線通信回線を介して接続可能な通信装置が検出された場合には、検出された通信装置から送信された情報を無線通信部２４によって受信して解析する。

【００３０】そして、受信した情報をメモリ２２内に格納された原始暗号化情報と照合し、一致した場合には接続を許可して、該検出された通信装置との間で無線通信を開始する。また、受信した情報が原始暗号化情報と一致しない場合には、該通信装置との間の通信を拒否する。

【００３１】メモリ２２は、ＥＥＰＲＯＭ、フラッシュメモリ等の不揮発性記憶素子を備えて構成される。メモリ２２は、ＣＰＵ２１により実行されるシステムプログラム等のプログラム、及び、これらプログラムに係るデータ等を格納する。また、メモリ２２は、ＣＰＵ２１により処理されるデータや、入力部２３から入力されたデータ等を一時的に保持する。

【００３２】ここで、メモリ２２に格納されるデータについて説明する。図２は、メモリ２２内部の構成を模式的に示す図である。メモリ２２内には、上記各種プログラムを格納した格納領域（図示略）の他、図２に示すように原始暗号化情報格納領域１０１及び転送諸元情報格納領域１０２が設けられる。

【００３３】原始暗号化情報格納領域１０１には、暗号化の際の「鍵」として使用される暗号化鍵情報、及び、暗号化鍵情報を他の電子機器に対して送信した履歴等を含む暗号化鍵管理情報が格納される。原始暗号化情報格納領域１０１に格納される各種情報を、原始暗号化情報と総称する。

【００３４】この原始暗号化情報格納領域１０１に格納される原始暗号化情報は、予め原始暗号化情報格納領域１０１に格納されているものとしても良いし、入力部２３の操作によって、随時入力されるようにしても良い。

【００３５】また、転送諸元情報格納領域１０２には、通信装置２の製品情報、固有機能情報、使用者情報、シリアルNo.等の各種情報が格納される。これらの転送諸元情報格納領域１０２に格納される各種情報を、転送諸元情報と総称する。なお、転送諸元情報格納領域１０２に格納される情報は、予めメモリ２２に格納されているものとしても良いし、入力部２３の操作によって入力されるものとしても良く、或いは、インターフェース部２８に接続された電子機器４から入力されるものとしても良い。

【００３６】入力部２３は、それぞれ入力可能な情報が割り当てられた複数のキー等の入力デバイスを備えており、操作内容に対応する操作信号を生成してＣＰＵ２１へ出力する。

【００３７】無線通信部２４は、エンコーダ、デコーダ、ＲＦ、アンプ等を内蔵しており、ＣＰＵ２１から入

力される信号を変換して無線信号を生成し、アンテナ２５を介して通信装置３へ送信する。また、無線通信部２４は、通信装置３から送信された無線信号をアンテナ２５によって受信し、受信した無線信号を変換して得られる信号をＣＰＵ２１へ出力する。

【００３８】ここで、無線通信部２４としては、例えば、ブルートゥース（Bluetooth）規格に準じた無線通信ユニットが挙げられる。Bluetooth規格とは、通信機器、電子機器、ソフトウェア等を製造する事業者が複数集まって構成されるプロモーターと、Bluetooth SIG（Special InterestGroup）により策定された無線通信規格である。Bluetooth規格では、2.4GHz（ギガヘルツ）帯の周波数の無線信号を利用して、およそ数メートル以内の複数の電子機器間で無線通信を行う。

【００３９】Bluetooth規格に準じた無線通信ユニットを搭載した電子機器は、互いにピコネットと呼ばれるグループを形成する。そして、同一のピコネットに属する電子機器間で相互に通信することが可能である。同一のピコネットには多くの電子機器が同時に属することができる。また、１台の通信装置が同時に複数のピコネットに属することも可能である。このため、携帯型電話機を始め、パーソナルコンピュータ、ＰＤＡ（Personal Digital Assistant）と呼ばれるハンドヘルドコンピュータ、プリンタ、音楽プレーヤ等の様々な機器を互いに接続する通信方式として注目されている。以下、無線通信部２４は上記Bluetooth規格に準じた通信ユニットであり、無線通信部２４及びアンテナ２５を利用して実行される無線通信（無線通信リンクＡを介した無線通信）は、Bluetooth規格に準じた2.4GHz帯の電波により行われるものとして説明する。

【００４０】赤外線通信部２６は、エンコーダ、デコーダ等を内蔵しており、赤外線受発光ユニット２７に接続されている。赤外線通信部２６は、ＣＰＵ２１から入力された信号を変換して赤外線受発光ユニット２７へ出力する。赤外線受発光ユニット２７は、ＬＥＤ（Light Emitting Diode）やフォトセンサ等を内蔵し、赤外線通信部２６から入力された信号をもとに内蔵するＬＥＤを発光させ、赤外線信号として通信装置３へ向けて出力する。

【００４１】また、赤外線受発光ユニット２７は、内蔵するフォトセンサによって通信装置３からの赤外光を受光すると、受光パターンを所定の信号に変換して赤外線通信部２６へ出力する。さらに、赤外線通信部２６は、赤外線受発光ユニット２７から入力される信号を変換して、ＣＰＵ２１へ出力する。

【００４２】インターフェース部２８は、通信装置２と、通信装置２の外部の電子機器とを接続するためのインターフェースであって、コネクタ等を備えている。ここで、インターフェース部２８に接続される電子機器５としては、例えば、携帯型電話機やパーソナルコンピュータ、ＰＤＡ等が挙げられるが、特に限定されるものではない。また、通信装置２は、図示しないリチウムイオン電池やニッケルーカドミウム電池等の二次電池、もしくは乾電池等を内蔵し、これらの電池を電源として動作するが、通信装置２に電池を内蔵せずに、インターフェース部２８を介して通信装置２へ電源が供給される構成としても良い。

【００４３】さらに、通信装置２が有する入力部２３に代えて、インターフェース部２８に接続された機器が具備する入力装置を用いる構成としても良い。この場合、ＣＰＵ２１は、インターフェース部２８に接続された機器から入力される信号に従って動作すれば良く、入力部２３を備えていなくても良い。

【００４４】次いで、通信装置３の構成について説明する。通信装置３は、ＣＰＵ３１、メモリ３２、入力部３３、無線通信部３４、アンテナ３５、赤外線通信部３６、赤外線受発光ユニット３７、及びインターフェース部３８の各部を備えて構成される。ここで、上記メモリ３２、入力部３３、無線通信部３４、アンテナ３５、赤外線通信部３６、赤外線受発光ユニット３７、及びインターフェース部３８の各部は、通信装置２が有するメモリ２２、入力部２３、無線通信部２４、アンテナ２５、赤外線通信部２６、赤外線受発光ユニット２７、及びインターフェース部２８の各部と同一の構成によってなるものであり、説明を省略する。

【００４５】ＣＰＵ３１は、入力部３３における指示操作に従って、メモリ３２に格納されたシステムプログラムを読み出して実行し、通信装置３の各部を駆動制御する。具体的には、ＣＰＵ３１は、メモリ３２内のプログラムに従って、無線通信部３４を制御し、通信装置２との間に無線通信リンクＡを確立する。

【００４６】続いてＣＰＵ３１は、赤外線通信部３６及び赤外線受発光ユニット３７によって赤外線通信リンクＢを確立する。そして、ＣＰＵ３１は、通信装置２が有する赤外線受発光ユニット２７から発せられた赤外線信号を赤外線受発光ユニット３７によって受光し、通信装置２から送信された暗号化に関する各種情報を受信する。

【００４７】ここで、ＣＰＵ３１は、通信装置２から送信された各種情報をメモリ３２内に格納するとともに、該情報を、赤外線通信部３６及び赤外線受発光ユニット３７を介して通信装置２へ送信する。そして、通信装置２が有するアンテナ２５から出力された無線信号を受信し、受信した信号が無線通信リンクＡ及び赤外線通信リンクＢの切断を要求している場合は、通信装置２との間の無線通信リンクＡ及び赤外線通信リンクＢを切断する。

【００４８】次に、本実施の形態の動作を説明する。図３は、本第１の実施の形態における通信システム１の動作を示すフローチャートである。図３（ａ）は、アクセ

ス要求側の装置、すなわち通信装置２の動作を示し、図３（ｂ）はアクセス受信側の装置、すなわち通信装置３の動作を示す。なお、図中、実線矢印で示す信号は、無線通信リンクＡ（図１）を介して送受信される上記Bluetooth規格に準じた無線信号であり、破線矢印で示す信号は、赤外線通信リンクＢ（図１）を介して送受信される赤外線信号である。

【００４９】まず、図３（ａ）に示すように、ＣＰＵ２１は、入力部２３からの指示入力に従って動作を開始し、通信装置３に対して接続を求める接続要求信号を生成して、無線通信部２４によって通信装置３へ送信させる（ステップＳ１１）。

【００５０】ＣＰＵ３１は、入力部３３からの指示入力によって動作を開始し、無線通信部３４によって通信装置２から送信される無線信号を受信可能な状態に移行する。そして、無線通信部２４から送信された接続要求を無線通信部３４によって受信すると（ステップＳ２１）、接続の確認となる接続確認信号を生成し、無線通信部３４によって送信させる（ステップＳ２２）。

【００５１】ＣＰＵ２１は、ＣＰＵ３１の制御により無線通信部３４から送信された接続確認信号を無線通信部２４によって受信すると（ステップＳ１２）、メモリ２２の転送諸元情報格納領域１０２に格納された転送諸元情報を読み出して、赤外線通信部２６及び赤外線受発光ユニット２７によって、赤外線信号として通信装置３へ送信させる（ステップＳ１３）。

【００５２】ＣＰＵ３１は、通信装置２の赤外線通信部２６により赤外線信号として送信された転送諸元情報を、赤外線通信部３６によって受信すると（ステップＳ２３）、メモリ３２の転送諸元情報格納領域１０２に格納された転送諸元情報を読み出して、赤外線通信部３６によって送信させる（ステップＳ２４）。

【００５３】ＣＰＵ２１は、通信装置３から送信された転送諸元情報を赤外線通信部２６によって受信すると（ステップＳ１４）、メモリ２２内の原始暗号化情報格納領域１０１に格納されている原始暗号化情報を読み出して、赤外線通信部２６によって通信装置３へ送信させる（ステップＳ１５）。

【００５４】ＣＰＵ３１は、通信装置２から送信された原始暗号化情報を受信すると（ステップＳ２５）、受信した原始暗号化情報をメモリ３２内の原始暗号化情報格納領域１０１に記憶させる（ステップＳ２６）。なお、ここで、予めメモリ３２の原始暗号化情報格納領域１０１に格納されていた原始暗号化情報については、新たに受信した原始暗号化情報により上書きされるものとしても良いし、或いは、新たに受信した原始暗号化情報とは異なる領域に保存されるものとしても良い。

【００５５】続いて、ＣＰＵ３１は、ステップＳ２５で受信し、メモリ３２内の原始暗号化情報格納領域１０１に記憶した原始暗号化情報を、赤外線通信部３６によって通信装置２へ送信する（ステップＳ２７）。

【００５６】ＣＰＵ２１は、通信装置３から送信された原始暗号化情報を受信すると（ステップＳ１６）、受信した原始暗号化情報と、メモリ２２の原始暗号化情報格納領域１０１に格納されている原始暗号化情報とを照合し、一致することを確認する（ステップＳ１７）。すなわち、ステップＳ１５で通信装置３へ送信した原始暗号化情報と、通信装置３から送信された原始暗号化情報とが一致することを確認することにより、ステップＳ１５，Ｓ１６，Ｓ２５，Ｓ２６における原始暗号化情報の送受信が問題なく実行されたことを確認する。

【００５７】そして、ＣＰＵ２１は、通信の切断を要求する切断要求信号を生成して、無線通信部２４によって通信装置３へ送信させる（ステップＳ１８）。ＣＰＵ３１は、通信装置２から送信された切断要求信号を無線通信部３４によって受信すると（ステップＳ２８）、切断要求の受信を確認する切断確認信号を生成して、無線通信部３４によって通信装置２へ送信させ（ステップＳ２９）、本処理を終了する。

【００５８】また、ＣＰＵ２１は、通信装置３から送信された切断確認信号を無線通信部２４によって受信すると（ステップＳ１９）、本処理を終了する。

【００５９】以上の図３に示す処理によって、通信装置２が有するメモリ２２と、通信装置３が有するメモリ３２とは、予めメモリ２２内の原始暗号化情報格納領域１０１に格納されていた原始暗号化情報を格納した状態になる。

【００６０】図３に示す処理においては、転送諸元情報および原始暗号化情報が、赤外線通信リンクＢ（図１）を介して送受信される。一般に、赤外線信号による無線通信を行う場合、通信を行う電子機器が互いに近接しており、かつ、互いの電子機器が有する赤外線受発光部が対向していることが必要である。特に、互いの電子機器が有する赤外線受発光部は、比較的狭い立体角に収まるように対向していなければならず、無関係な電子機器により傍受される可能性は低く、セキュリティ上の懸念は小さいものである。しかしながら、以下に述べる暗号化を施すことにより、赤外線通信リンクＢを介した通信におけるセキュリティ上の信頼性をより確実なものとすることができる。

【００６１】図４（ａ）には、暗号化を施す際の赤外線通信におけるプロトコル構成を示す階層モデルを図示する。また、図４（ｂ）には、赤外線通信におけるデータユニットの構成を模式的に示す。

【００６２】一般に、赤外線通信においては、データリンク層、リンクマネージメント層、トランスポート層における互換性を保持していれば、それより上位の階層におけるサービス・データ・ユニットを暗号化しても、プロトコル互換性を保つことができる。従って、図４（ａ）に示すように、トランスポート層よりも上位の層

を暗号化層とし、さらにその上位層を、前述の転送諸元情報や原始暗号化情報を交換するセキュリティデータ交換プロトコル層とすれば、プロトコル互換性を保ちながら、転送される情報の秘匿性を保つことができる。

【００６３】具体的には、図４（ｂ）に示すように、ＬＡＰ（データリンク層）、ＬＭＰ（リンクマネージメント層）、及びＴＰ（トランスポート層）のプロトコルデータユニットに続くサービス・データ・ユニットを暗号化すれば良い。従って、通信装置２及び通信装置３の双方において、赤外線通信リンクＢを介して送受信する信号の暗号化及び復号を行うことにより、図３に示す処理で送受信される転送諸元情報や原始暗号化情報の秘匿性をより確実なものとすることができる。

【００６４】図５は、図３に示す処理の実行後における通信装置２の動作を示すフローチャートである。この図５に示す処理において、通信装置２は、Bluetooth規格により規定されるMasterのデバイスとして動作する。また、図５に示す処理において送受信される無線信号は、Bluetooth規格に準じた2.4GHz帯の無線信号である。

【００６５】まず、ＣＰＵ２１は、入力部２３から入力される指示に従って動作を開始し、無線通信部２４を制御してPage Scan動作を実行し、Bluetooth規格に準じた通信が可能な通信装置を検出する（ステップＳ４１）。

【００６６】そして、接続可能な通信装置を検出した場合は、ＣＰＵ２１によるPage Scan動作に応じて検出した装置から送信された情報を受信し（ステップＳ４２）、受信した情報と、メモリ２２内の原始暗号化情報格納領域１０１に格納されている原始暗号化情報との照合を行う（ステップＳ４３）。

【００６７】ここで、通信装置２が通信装置３を検出した場合、通信装置３は、メモリ２２内の原始暗号化情報格納領域１０１に格納されている原始暗号化情報を既に保持しているため、Page Scan動作に応じて原始暗号化情報に従って暗号化された情報を送信する。また、通信装置２及び通信装置３とは無関係な通信装置が検出された場合は、この無関係な通信装置からは、Page Scan動作に応じて通常の無線信号が送信される。従って、ステップＳ４３における照合により、ステップＳ４１で検出した通信装置が通信装置３であるか否かを判別できる。

【００６８】ステップＳ４３における照合の結果、ステップＳ４２で受信した無線信号が原始暗号化情報とは無関係であった場合は（ステップＳ４４；Ｎｏ）、ＣＰＵ２１は、検出した通信装置との接続を拒否し（ステップＳ４５）、本処理を終了する。

【００６９】また、ステップＳ４３での照合により、ステップＳ４２で受信した無線信号が原始暗号化情報に適合した場合は（ステップＳ４４；Ｙｅｓ）、ＣＰＵ２１は、検出した通信装置との間で、原始暗号化情報格納領域１０１内の原始暗号化情報により暗号化された無線信号の送受信を開始する（ステップＳ４６）。なお、原始暗号化情報格納領域１０１に格納された原始暗号化情報により暗号化された情報は、該原始暗号化情報をもとに復号できる。このため、ＣＰＵ２１は、無線通信部２４により送信する情報を暗号化するとともに、無線通信部２４により受信した情報を復号する。

【００７０】そして、ＣＰＵ２１は、検出した通信装置との間のネゴシエーションが終了してからアプリケーションでの使用を許可する（ステップＳ４７）。その後、ＣＰＵ２１は、通信装置２、もしくはインターフェース部２８に接続された電子機器４上で実行されるアプリケーションプログラムの要求に応じて、暗号化された無線信号を送受信する処理を実行し（ステップＳ４８）、入力部２３からの指示入力によって本処理を終了する。

【００７１】以上のように、本発明の第１の実施の形態によれば、Bluetooth規格に準じた無線通信を行う無線通信部２４及びアンテナ２５と、赤外線信号を用いた無線通信を行う赤外線通信部２６及び赤外線受発光ユニット２７とを備える通信装置２と、通信装置２と同一構成によってなる通信装置３との間において、予め赤外線通信によって原始暗号化情報を転送し、その後、転送した原始暗号化情報に基づいて暗号化された情報を、Bluetooth規格に準じた無線通信で送受信する。これにより、高い秘匿性を保ちながら、Bluetooth規格に準じた利便性の高い通信を行うことができる。

【００７２】すなわち、Bluetooth規格に準じた無線通信を利用した場合、互いの通信装置を近接させるだけでピコネットを形成して通信を開始できる。また、通信中の各通信機器は、同時に他の通信装置との間においてピコネットを形成することができ、フレキシブルな通信を行うことができる。さらに、ピコネットを形成する通信装置は、互いに所定の距離以内に近接していれば良く、位置が拘束されることが少ない。その反面、Bluetooth規格に準じた無線通信では、特定の通信装置に対してのみ情報を送信することが難しく、誤って無関係な通信装置に受信されてしまう可能性が否定できない。しかしながら、上記第１の実施の形態における通信システム１によれば、予め通信装置２と通信装置３との間で、赤外線通信によって原始暗号化情報を転送することにより、無関係な通信装置に影響されることなく原始暗号化情報を共有し、この原始暗号化情報を用いて暗号化された情報を、Bluetooth規格に準じた無線通信で送受信する。従って、セキュリティ上の信頼性を確保しながら、利便性の高い無線通信を行うことができる。

【００７３】なお、上記実施の形態においては、通信装置２と通信装置３とは、Bluetooth規格に準じた無線通信リンクＡを介して無線通信を行うものとしたが、本発明はこれに限定されるものではなく、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に対しても適用可能であり、上記の通信システム１と同様の効果を奏するものである。

15

【００７４】さらに、携帯型電話機やＰＤＡ、パーソナルコンピュータ、プリンタ、音楽プレーヤ等の各種電子機器に本発明を適用する場合は、図１に示したような通信装置２及び通信装置３に対して電子機器４，５が接続される構成に限らず、上記各種電子機器に、通信装置２，３の機能を内蔵させることも勿論可能である。

【００７５】また、上記第１の実施の形態においては、通信装置２及び通信装置３はいずれも入力部２３，３３を具備しており、これら入力部２３，３３における指示入力によって図３に示す処理を開始するものとしたが、必ずしも入力部２３，３３を備える構成でなくても良い。以下、この場合について第２の実施の形態として説明する。

【００７６】〔第２の実施の形態〕図６は、本発明の第２の実施の形態における通信システム１０の構成を示すブロック図である。

【００７７】同図に示すように、通信システム１０は、通信装置２と、通信装置３ａとによって構成される。通信システム１０は、通信装置３ａが有するメモリ６１およびスイッチ６２を除いては、上記第１の実施の形態における通信システム１と同様の構成によってなるものであり、共通部分については同符号を付して説明を省略する。

【００７８】スイッチ６２は、１個もしくは複数のスイッチを備えており、操作される毎に操作信号を生成してＣＰＵ３１へ出力する。

【００７９】図７は、メモリ６１の内部構成を模式的に示す図である。同図に示すように、メモリ６１内には、原始暗号化情報格納領域１０３及び転送諸元情報格納領域１０２が設けられており、転送諸元情報格納領域１０２には製品情報、固有機能情報、使用者情報、シリアルNo.等の転送諸元情報が格納されている。一方、原始暗号化情報格納領域１０３には、事前に原始暗号化情報は格納されていない。

【００８０】上記第１の実施の形態で説明した通信システム１では、図３に示す処理において、通信装置２から通信装置３へ原始暗号化情報が転送され、メモリ２２の原始暗号化情報格納領域１０１に格納されていた原始暗号化情報が、メモリ３２の原始暗号化情報格納領域１０１に格納される。本第２の実施の形態における通信システム１０では、通信装置２から通信装置３ａへ原始暗号化情報が転送されると、転送された原始暗号化情報はメモリ６１の原始暗号化情報格納領域１０３へ格納される。従って、通信装置３ａは、上記通信装置３と同様に動作することができる。

【００８１】また、上記第１の実施の形態で説明した通信システム１では、通信装置２が有する入力部２３および通信装置３が有する入力部３３における指示入力により、図３に示す処理が開始されるものとした。本第２の実施の形態における通信システム１０では、通信装置２が有する入力部２３における指示入力、及び、通信装置３ａが有するスイッチ６２のスイッチ操作によって、図３に示す処理と同様の処理が実行される。

16

【００８２】すなわち、通信装置３ａは、入力手段としてスイッチ６２のみを備える装置であるが、上記第１の実施の形態における通信装置３に代えて、通信装置２によるアクセスを受信する動作のみを行う装置として使用可能である。また、通信装置２に代えてアクセス要求側の装置として利用しないため、メモリ６１の原始暗号化情報格納領域１０３には予め原始暗号化情報を格納する必要がない。

【００８３】従って、本第２の実施の形態における通信システム１０は、入力スイッチ６２のみを有する通信装置３ａを用いて、上記第１の実施の形態と同様の効果を奏するものである。これにより、Bluetooth規格に準じた無線通信において、Slaveのデバイスとしてのみ機能する装置には、入力手段としては単なるスイッチを備えるだけで、通信システム１と同様の効果を得ることができる。

【００８４】

【発明の効果】請求項１記載の発明の通信装置によれば、送信される情報は、第２の通信手段によって送信された暗号化鍵情報を受信した通信装置でのみ受信可能となる。これにより、第１の通信手段による無線通信について、セキュリティ上の信頼性を確保することができる。特に、第１の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第２の通信手段によって送信される暗号化鍵情報を受信した通信装置のみに限定できる。従って、通信相手の装置との位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

【００８５】請求項２記載の発明の通信装置によれば、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、通信拒否手段により、第１の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置を厳格に限定し、情報の秘匿をより確実に保持することができる。

【００８６】請求項３記載の発明の通信装置によれば、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース（Bluetooth）規格の無線通信において、情報の秘匿性を確保することができる。特に、第２の通信手段に赤外線信号を用いた通信方式を利用するので、第２の通信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能であ

17

る。また、赤外線信号を用いた通信方式では、通信装置は互いに近接し、かつ所定の立体角以内で対向する必要があるので、情報の秘匿性をより一層高めることができる。

【００８７】請求項４記載の発明の通信システム、及び、請求項８記載の発明の通信方法によれば、送信側装置により送信される情報は受信側装置でのみ受信することができる。これにより、送信側装置が有する第１の通信手段を用いた通信システム内の無線通信について、セキュリティ上の信頼性を確保することができる。特に、第１の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第２の通信手段によって送信される暗号化鍵情報を保持する受信側装置のみに限定できる。従って、互いの装置の位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

【００８８】請求項５記載の発明の通信システムによれば、送信側装置は、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、受信側装置が有する受信鍵情報保持手段に保持されていない場合に、通信拒否手段によって、第１の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置をより厳格に限定し、情報の秘匿をより確実に保持することができる。

【００８９】請求項６記載の発明の通信システムによれば、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース（Bluetooth）規格の無線通信において、情報の秘匿性を確保することができる。特に、第２の通信手段と鍵情報受信手段とは赤外線信号を用いた通信方式を利用するので、第２の通信手段および鍵情報受信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能である。また、赤外線信号を用いた通信方式では、送信側装置と受信側装置とは互いに近接し、かつ所定の立体角以内で対向する必要があるので、情報の秘匿性をより一層高めることができる。

18

【００９０】請求項７記載の発明の通信システムによれば、送信側装置が有する鍵情報送信制御手段は、暗号化鍵情報を暗号化して第２の通信手段によって送信させるので、暗号化鍵情報を送信する際の情報の漏洩をより確実に防止できる。これにより、セキュリティ上の信頼性をより一層高めることができる。

【図面の簡単な説明】

【図１】本発明を適用した第１の実施の形態における通信システム１の構成を示すブロック図である。

【図２】図１のメモリ２２，３２の内部構成を模式的に示す図である。

【図３】図１の通信システム１の動作を示すフローチャートであり、（ａ）は通信装置２の動作を示し、（ｂ）は通信装置３の動作を示す。

【図４】図３に示す処理に暗号化を施した場合のプロトコル構成を示す説明図であり、（ａ）は暗号化を施す際の赤外線通信におけるプロトコル構成を示す階層モデルを示し、（ｂ）は、赤外線通信におけるデータユニットの構成を模式的に示す。

【図５】図１の通信装置２によりBluetooth規格に準じた無線通信を行う際の動作を示すフローチャートである。

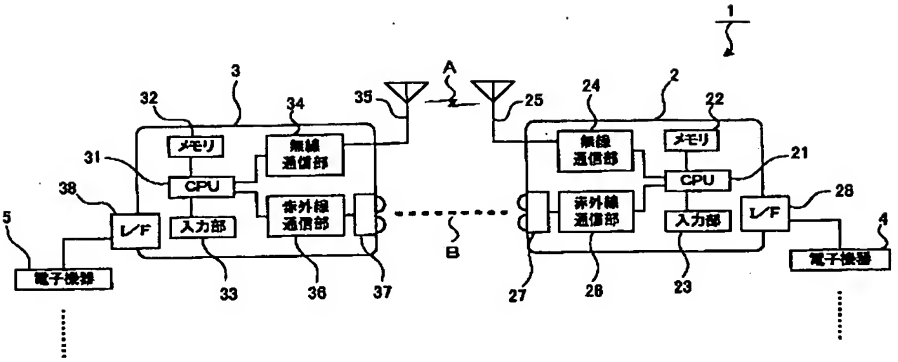
【図６】本発明を適用した第２の実施の形態における通信システム１０の構成を示すブロック図である。

【図７】図６に示すメモリ６１の内部構成を模式的に示す図である。

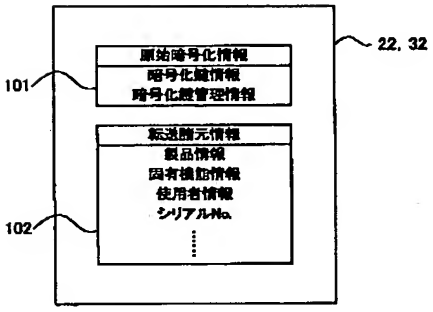
【符号の説明】

１，１０　通信システム
２，３　通信装置
２１，３１　ＣＰＵ
２２，３２　メモリ
２３，３３　入力部
２４，３４　無線通信部
２５，３５　アンテナ
２６，３６　赤外線通信部
２７，３７　赤外線受発光ユニット
２８，３８　インターフェース部
６１　メモリ
６２　スイッチ
１０１，１０３　原始暗号化情報格納領域
１０２　転送諸元情報格納領域

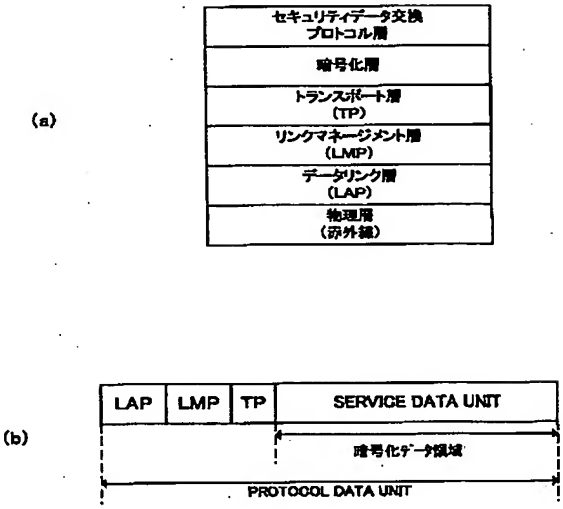
【図１】


1
A
B
3
2
メモリ
CPU
無線通信部
赤外線通信部
入力部
レ/F
電子機器
31
32
33
34
35
36
37
38
5
4
22
23
24
25
26
27
28

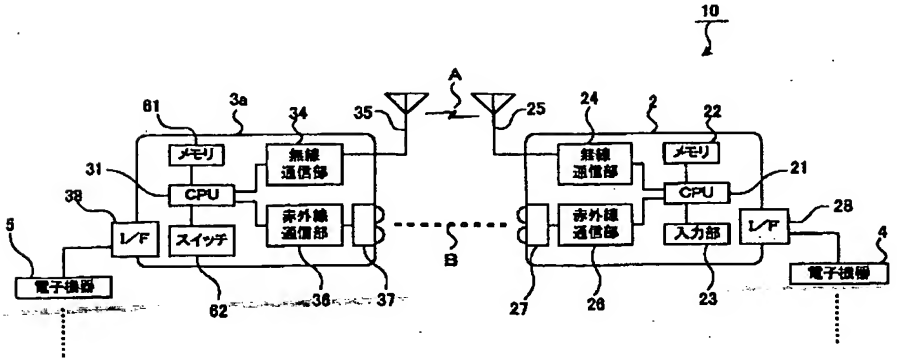
【図２】


22, 32
101
原始暗号化情報
暗号化鍵情報
暗号化鍵管理情報
102
転送前元情報
製品情報
固有機能情報
使用者情報
シリアルNo.

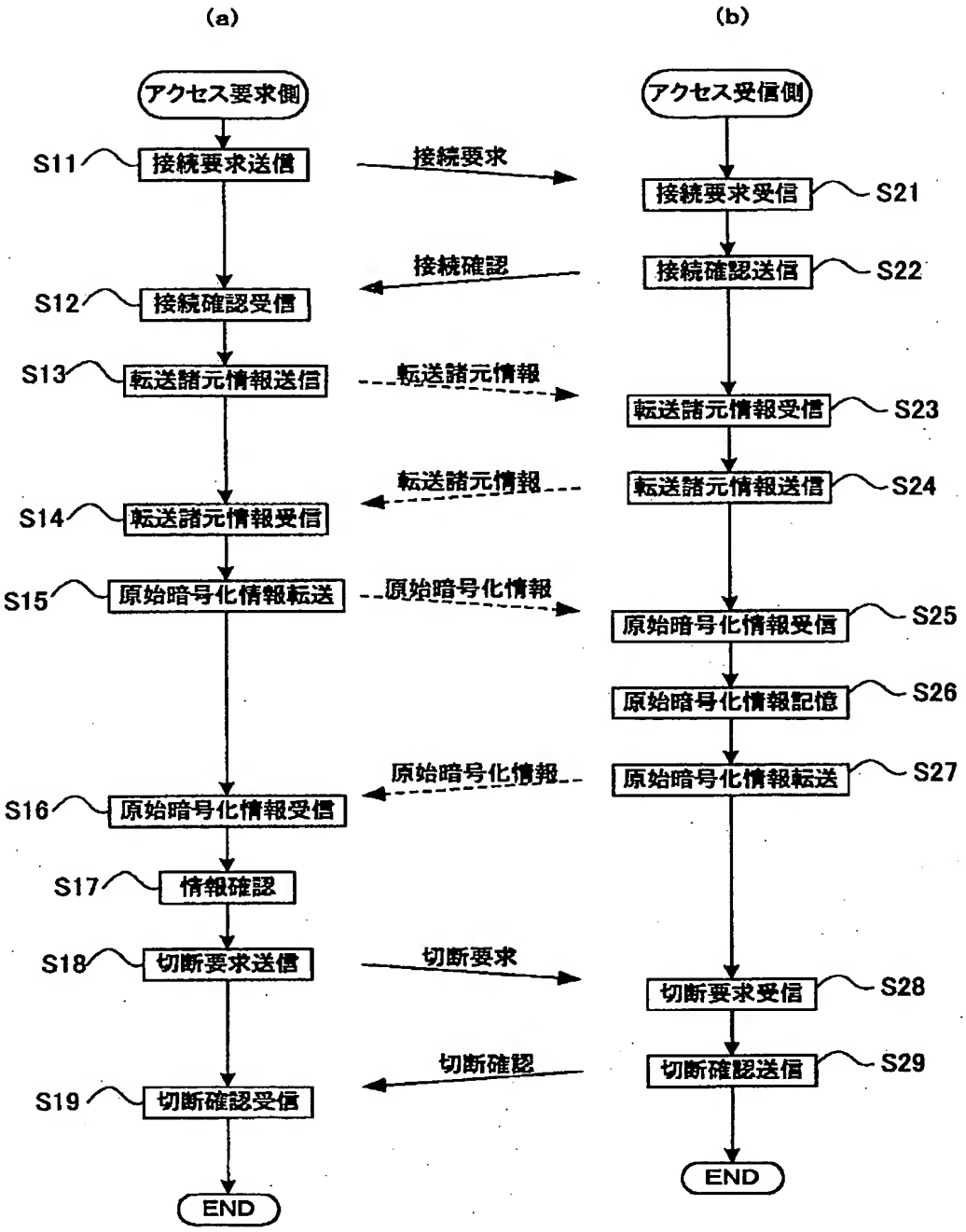
【図４】


(a)
セキュリティデータ交換プロトコル層
暗号化層
トランスポート層 (TP)
リンクマネージメント層 (LMP)
データリンク層 (LAP)
物理層 (赤外線)
(b)
LAP
LMP
TP
SERVICE DATA UNIT
暗号化データ領域
PROTOCOL DATA UNIT

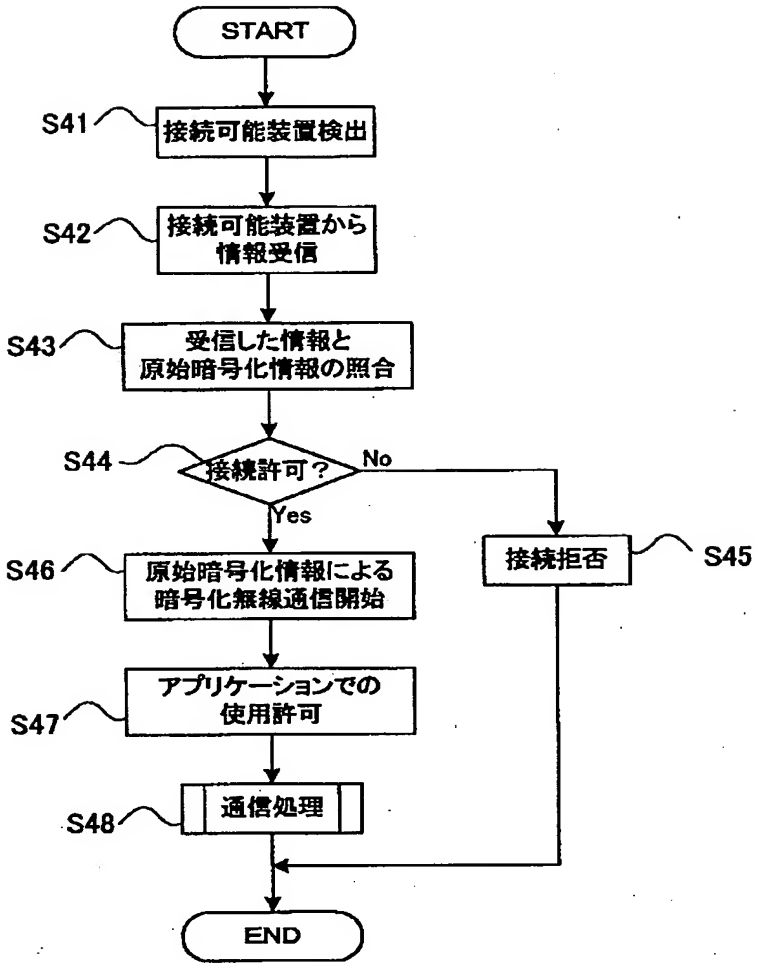
【図６】


10
A
B
61
3a
62
メモリ
CPU
無線通信部
赤外線通信部
スイッチ
入力部
レ/F
電子機器
31
34
35
36
37
38
5
4
22
23
24
25
26
27
28

【図３】


(a)
(b)
アクセス要求側
アクセス受信側
S11
接続要求送信
接続要求
接続要求受信
S21
接続確認
S12
接続確認受信
接続確認送信
S22
S13
転送諸元情報送信
転送諸元情報
転送諸元情報受信
S23
転送諸元情報
S14
転送諸元情報受信
転送諸元情報送信
S24
S15
原始暗号化情報転送
原始暗号化情報
原始暗号化情報受信
S25
原始暗号化情報記憶
S26
原始暗号化情報
S16
原始暗号化情報受信
原始暗号化情報転送
S27
S17
情報確認
S18
切断要求送信
切断要求
切断要求受信
S28
切断確認
S19
切断確認受信
切断確認送信
S29
END
END

【図５】


START
S41
接続可能装置検出
S42
接続可能装置から
情報受信
S43
受信した情報と
原始暗号化情報の照合
S44
接続許可？
No
Yes
S45
接続拒否
S46
原始暗号化情報による
暗号化無線通信開始
S47
アプリケーションでの
使用許可
S48
通信処理
END

【図７】